

JOSEPH W. PRICE  
ALBIN H. GESS  
FRANKLIN D. UBELL  
MICHAEL J. MOFFATT  
GORDON E. GRAY III  
BRADLEY D. BLANCHE

# PRICE, GESS & UBELL

ATTORNEYS AT LAW

2100 S.E. MAIN STREET, SUITE 250

IRVINE, CALIFORNIA 92614-6238

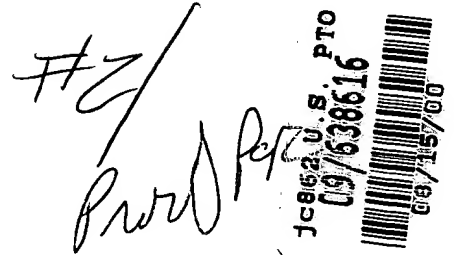
A PROFESSIONAL CORPORATION

TELEPHONE: (949) 261-8433

FACSIMILE: (949) 261-9072

FACSIMILE: (949) 261-1726

e-mail: pgu@pgulaw.com



**PRIORITY DOCUMENT - JAPAN 11-245277**

Applicant(s):

Makoto Tatebayashi et al.

Title:

ENCRYPTION METHOD, ENCRYPTION  
APPARATUS, DECRYPTION METHOD, AND  
DECRYPTION APPARATUS

Attorney's

Docket No.:

NAK1-BM08

**"EXPRESS MAIL" MAILING**  
**LABEL NO. EL230379070US**

**DATE OF DEPOSIT: August 15, 2000**

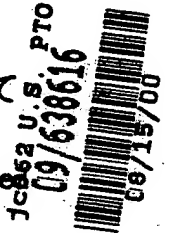
日本国特許庁

PATENT OFFICE  
JAPANESE GOVERNMENT

J.W. PRICE 949/261.8433  
MAKOTO TATEBAYASHI et al  
NAK2-BM08

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.



出願年月日

Date of Application:

1999年 8月31日

出願番号

Application Number:

平成11年特許願第245277号

出願人

Applicant(s):

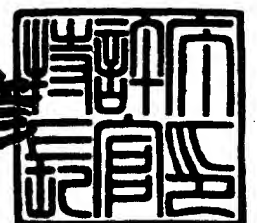
松下電器産業株式会社  
株式会社東芝

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 6月 9日

特許庁長官  
Commissioner,  
Patent Office

近藤 隆彦



出証番号 出証特2000-3043276

【書類名】 特許願

【整理番号】 2022510387

【提出日】 平成11年 8月31日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 9/06

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 館林 誠

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 横田 薫

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 大森 基司

【発明者】

【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

【氏名】 佐野 文彦

【発明者】

【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

【氏名】 遠藤 直樹

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【選任した代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9810105

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ暗号化装置及び暗号処理方法

【特許請求の範囲】

【請求項 1】 入力データを N ビット単位の入力ブロックに分割し、予め与えられた鍵データに基づいて、順次前記入力ブロックを所定のアルゴリズムに従って暗号化し暗号化ブロックとし、前記暗号化ブロックを連結し暗号文データとして出力するデータ暗号化装置であって、

予め初期データが設定されていて、ある入力ブロックに先立ってデータ出力された暗号化ブロックを記憶し、予め設定されている所定の入力ブロックに対して暗号化を行うときには記憶データを前記初期値に初期化するデータ記憶手段と、

前記データ記憶手段の記憶データを所定の変換で変換するデータ変換手段と、

前記データ変換手段から出力されたデータと前記鍵データを融合するデータ融合手段と、

前記所定の入力ブロックに対して暗号化を行う時は前記データ融合手段から出力されたデータに基づいて第 1 の部分鍵生成処理を行い、前記所定の入力ブロック以外の入力ブロックに対して暗号化を行う時は前記データ融合手段から出力されたデータに基づいて第 2 の部分鍵生成処理を行う部分鍵生成手段と、

前記部分鍵生成手段から出力されたデータに基づいて入力ブロックを暗号化して暗号化ブロックとして出力するデータ暗号化手段とを備え、

前記部分鍵生成手段で行う前記第 1 の部分鍵生成処理と前記第 2 の部分鍵生成処理は安全性のための処理負荷を異ならせていることを特徴とするデータ暗号化装置。

【請求項 2】 前記第 2 の部分鍵生成処理は、前記データ融合手段から出力されたデータに基づいてデータを生成し、前記生成されたデータと同じデータ複数個をビット連結することによって行い、これにより、前記第 1 の部分鍵生成手段よりも安全性のための処理負荷を小さくしていることを特徴とする請求項 1 記載のデータ暗号化装置。

【請求項 3】 前記データ融合手段におけるデータ融合操作は、ビット毎の排他的論理和、または加算演算とすることを特徴とする請求項 1 記載のデータ暗号

化装置。

【請求項 4】 前記所定の入力ブロックは、M 番目毎に入力される入力ブロックであって、前記数値 M は 2 以上の整数であることを特徴とする、請求項 1 記載のデータ暗号化装置。

【請求項 5】 入力データを N ビット単位の入力ブロックに分割し、予め与えられた鍵データに基づいて、順次前記入力ブロックに対して所定の暗号化処理を施し暗号化ブロックとし、前記暗号化ブロックを連結し暗号文データとして出力する暗号処理方法であって、

記憶手段が、ある入力ブロックに先立ってデータ出力された暗号化ブロックを記憶しており、

所定の入力ブロックの暗号処理を行う時は、記憶手段に記憶された連鎖データを所定の初期値に初期化する初期化ステップと、

記憶手段に記憶されている連鎖データを所定の変換で変換し変換データを生成するデータ変換ステップと、

変換データと鍵データを融合して融合データを生成する融合ステップと、

前記所定の入力ブロックの暗号処理を行う時は、前記融合データに基づいて第 1 部分鍵生成処理を行って部分鍵データを生成し、前記所定の入力ブロック以外  
の入力ブロックの暗号処理を行う時は、前記融合データに基づいて第 2 部分鍵生成処理を行って部分鍵データを生成する部分鍵生成ステップと、

部分鍵データに基づいて入力ブロックを暗号化し暗号化データを生成して暗号化ブロックとして出力する暗号化ステップと、

暗号化ステップで生成された暗号化データを新たな連鎖データとして記憶手段に記憶された連鎖データを更新し、次の暗号処理に供させる記憶ステップとを備え、

前記第 1 部分鍵生成処理と前記第 2 部分鍵生成処理とは安全性のための処理負荷を異ならせていることを特徴とする暗号処理方法。

【請求項 6】 前記第 2 部分鍵生成処理は、融合データに基づいてデータを生成し、前記生成されたデータと同じデータ複数個をビット連結することによって部分鍵生成処理を行い、これにより前記第 1 部分鍵生成処理よりも安全性のため

の処理負荷を小さくしていることを特徴とする、請求項 5 記載の暗号処理方法。

【請求項 7】 前記データ融合ステップにおけるデータ融合操作は、ビット毎の排他的論理和または加算演算とすることを特徴とする請求項 5 記載の暗号処理方法。

【請求項 8】 前記所定の入力ブロックは、入力される M 番目毎の入力ブロックであって、前記数値 M は 2 以上の整数であることを特徴とする請求項 5 記載の暗号化処理方法。

#### 【発明の詳細な説明】

#### 【0001】

#### 【発明の属する技術分野】

本発明は、秘密鍵に基づいて、被暗号処理データをブロック単位で暗号化する暗号処理装置及び暗号処理方法であって、特に処理速度を大幅に低下させることなく安全性を向上させる技術に関する。

#### 【0002】

#### 【従来の技術】

近年、デジタル通信が急速に普及してきたが、健全な産業の発展やプライバシーを保護する等の観点から、通信におけるデータの機密性を確保できる安全性の高いデータ暗号化方式が要求されている。また、暗号化方式に対しては、安全性のみならず暗号処理の高速性及びハードウェア／ソフトウェア両面における実装の簡便性も要求される。

#### （第 1 の従来例）

データ暗号化方式の第 1 の従来例として、擬似乱数加算型暗号がある。

#### 【0003】

この方式では、送信側・受信側双方が同じ秘密鍵（以下、単に「鍵」という。）を共有しており、平文データ M を一定長の平文データブロック  $M_i$  に区切り、区切られた各  $M_i$  に対して、共有している鍵をシードとして平文データブロック  $M_i$  と同じ長さの乱数データ R を発生させる。そして、各平文データブロック  $M_i$  とその乱数データ R とを対応させるビット毎に排他的論理和の計算を行うことによって、暗号文データブロック  $C_i$  を得る。式に表現すると以下の通りである

## 【0 0 0 4】

$$C_i = M_i (+) R$$

ただし、演算子“(+)”は対応するビット毎の排他的論理和を意味する。

最後に、得られた各暗号文データブロック  $C_i$  を連結し、暗号文  $C$  が得られるというものである。

この方式は、暗号化速度が非常に高いという点が特徴であり、画像や音声データのリアルタイム通信におけるデータ暗号化方式として適している。

## 【0 0 0 5】

しかし、この方式は既知平文攻撃に対してきわめて安全性が低い。すなわち、いま暗号化する鍵の値が同じであるとする、わずか1組の平文データブロック  $M_i$  と暗号文データブロック  $C_i$  を入手しただけで、以下の式より、乱数  $R$  が判明するので、他の全ての平文データブロック  $M_i$  を解読することができてしまう。

## 【0 0 0 6】

$$R = M_i (+) C_i$$

(第2の従来例)

データ攪乱の能力が高い暗号方式としては、ブロック暗号方式というものがある。ブロック暗号方式の具体例としては、DES (Data Encryption Standard) 方式やFEAL (Fast Data Encipherment Algorithm) 方式といったものがある。

DES方式では、64ビットの平文ブロックを56ビットの鍵を用いて暗号化し、64ビットの暗号文ブロックに変換する。実際の暗号化では、56ビットの鍵データを元に生成される48ビット×16個の部分鍵データを用いる。64ビット以上の平文に対しては、64ビットのブロックに分割して、暗号化を行う。DES方式ならびにFEAL方式は、岡本栄司著「暗号理論入門」(共立出版)に詳しく述べられている。

(第3の従来例)

第2の従来例であげたブロック暗号方式に対する代表的な解読法として、差分



解読法と線形解読法というものがある。第3の従来例はこれらの解読法に対する安全性を強化する目的で考案された暗号方式である。なお、差分解読法・線形解読法の詳細については、それぞれE. Biham, A. Shamir 著, 'Differential Cryptanalysis of the Data Encryption Standard,' Springer-Verlag. 及び松井充著, 'DES暗号の線形解読法(I),' 1993年暗号と情報セキュリティシンポジウム(SCIS'93)予稿集SCIS93-3C. に記載されている。

## 【0007】

差分解読法・線形解読法のいずれにおいても、同一の鍵で暗号化された平文-暗号文ペアを多数用意し、それらを解析することによって暗号化に使用されている鍵を求めるというものである。暗号解読を成功させるためには、同一の鍵データで暗号化された平文-暗号文ペアが多数必要になる。よって、複数の平文ブロックを暗号化する場合に、ブロック毎に異なる鍵データを用いて暗号化を行えば、これらの解読法に対する安全性は強化される。そこで、一つ前の平文ブロックの暗号化から得られる「可変情報」を利用して鍵データを更新していくという方式が考案されている。

## 【0008】

ここでは、第3の従来例として特開平11-7239号公報にある鍵連鎖方式を挙げる。この方式では、「可変情報」として1つ前の暗号化で得られる暗号文データを用いて鍵データの更新を行っている。

図6はこの方式のデータ暗号化装置40の内部構成を示すブロック図である。

データ暗号化部400は、データ暗号化部400の外部から入力される1ブロック(64ビット)の平文データを、部分鍵データ生成部401から入力される部分鍵データ32ビット×16に従って暗号化し、その結果得られる暗号文データ64ビットを出力する。

## 【0009】

部分鍵データ生成部401は、排他的論理和部402から入力される入力鍵データ64ビットをもとに32ビット×16の部分鍵データを生成し、データ暗号

化部 4 0 0 に入力する。

排他的論理和部 4 0 2 は、データ暗号化部 4 0 0 の外部から入力される暗号化鍵データ 6 4 ビットとデータ変換部 4 0 3 から入力される 6 4 ビットデータとのビット毎の排他的論理和演算を行い、演算結果を入力鍵データ 6 4 ビットとして出力する。

【0 0 1 0】

データ変換部 4 0 3 は、レジスタ 4 0 4 から入力される 6 4 ビットデータに対して所定の変換操作を行い、結果の 6 4 ビットデータを出力する。

レジスタ 4 0 4 は、予め設定された初期値によって初期化されており、1 ブロック前の平文の暗号化で得られた 6 4 ビット暗号文データを保管し、次の平文ブロックの暗号化の際に、その保管している 6 4 ビットデータを出力しデータ変換部 4 0 3 に入力する。

【0 0 1 1】

次に、暗号化する時の動作について述べる。

入力されるデータは 6 4 ビットのブロック単位に先頭から  $P_0$ ,  $P_1$ , ... に分割される。そして  $P_0$  から順に 6 4 ビットの平文データとして、データ暗号化装置 4 0 に入力され、6 4 ビットの暗号化鍵データに従い暗号化される。データ暗号化装置 4 0 では、入力される 6 4 ビットの平文データ  $P_t$  ( $t = 0, 1, \dots$ ) に対して、以下のような暗号化処理が行われる。

【0 0 1 2】

最初に、データ変換部 4 0 3 は、レジスタ 4 0 4 に保管されている 1 つ前の暗号文データ  $C(t-1)$  をデータ変換し、その変換された 6 4 ビットデータ  $f(C(t-1))$  を排他的論理和部 4 0 2 に入力する。ただし、 $t = 0$  の時には、レジスタ 4 0 4 からはレジスタの初期値  $IV$  が入力され、その変換データ  $f(IV)$  を出力する。排他的論理和部 4 0 2 はデータ変換部 4 0 3 より入力される前記 6 4 ビットデータ  $f(C(t-1))$  と、前記 6 4 ビットの暗号化鍵データとの排他的論理和演算を行い、その結果の 6 4 ビットデータを入力鍵データとして出力する。

【0 0 1 3】

次に部分鍵データ生成部 4 0 1 では、排他的論理和部 4 0 2 から入力される前記 6 4 ビット入力鍵データを元に 3 2 ビット×1 6 の部分鍵データを生成し、データ暗号化部 4 0 0 に入力する。

データ暗号化部 4 0 0 では、データ暗号化装置 4 0 の外部から入力される 6 4 ビットの平文データ  $P_t$  に対して、部分鍵データ生成部 4 0 1 から入力される前記 6 4 ビットの部分鍵データ 3 2 ビット×1 6 に従い、所定の暗号化処理を行ってその結果得られる 6 4 ビットデータを  $C_t$  とする。そして、データ暗号化装置 4 0 は  $C_t$  を出力する。

#### 【0 0 1 4】

データ暗号化部 4 0 0 および部分鍵データ生成部 4 0 1 の具体的な処理内容としては、第 2 の従来例の説明の中で挙げた D E S 暗号方式、F E A L 暗号方式、といったブロック暗号方式の暗号化部分および部分鍵生成部分をそれぞれ用いる。

この方式では、6 4 ビット以上の平文を複数ブロックに分けて暗号化する場合、各平文ブロックの暗号化毎に、入力鍵データが更新される。すなわち、各平文ブロックで異なる入力鍵データを用いて暗号化されるので、解読者は、次のようにして、同一の鍵で暗号化された平文-暗号文のペアを集めるしかない。

#### 【0 0 1 5】

すなわち、平文データ系列の先頭ブロック  $P_0$  の暗号化では、同じ入力鍵データ（すなわち  $f(I V)$  と鍵データとを排他的論理和演算した値）が部分鍵データ生成部 4 0 1 に入力されることが保証できるので、各平文データ系列の先頭ブロック  $P_0$  とそれに対応する暗号文データ  $C_0$  を収集することで所要の平文・暗号文ペアを得ることができる。通常、暗号化を行う平文データ系列は、画像・音声データといった膨大なデータ量を有するので、前記の方法で多数の既知平文・暗号文ペアを集めることは、平文の全てのブロックに対して同一の鍵データで暗号化を行う第 2 の従来例と比べて困難になる。

#### 【0 0 1 6】

従って、第 3 の従来例は、前記の差分解読法・線形解読法といった既知平文攻撃に対する安全性が強化されている。

【0 0 1 7】

【発明が解決しようとする課題】

しかしながら、この第3の従来例においては、平文データ1ブロックを暗号化する毎に部分鍵データ生成部401は、入力鍵データから部分鍵データを生成する処理を行わなければならない、暗号化の処理速度が低下するという問題がある。

例えば、データ暗号化部400および部分鍵データ生成部401に前述のFEAL暗号方式を適用するとする。FEAL暗号方式の部分鍵データ生成部はデータ暗号化部と同程度の処理量を必要とする。通常のFEAL暗号方式では、1つの平文データを暗号化する場合に、部分鍵生成は1度行うだけでよいので、画像・音声データなどのデータ長の長い平文データを暗号化する場合には、部分鍵生成処理による速度の低下は無視できるほど小さくなる。

【0 0 1 8】

しかし、FEAL暗号方式を第3の従来例に用いて暗号化を行う場合には、ブロック毎に部分鍵生成を実行するので、普通にFEAL暗号方式で暗号化を行うよりも暗号化速度が約1/2に低下する。一般に、ブロック暗号方式における鍵生成部はデータ暗号化部と同程度あるいはそれ以上の処理量を必要とするので、上記のような問題はFEAL暗号方式の場合に限らず、他のブロック暗号方式についても同様の問題が生じる。

【0 0 1 9】

一方、従来例3において部分鍵データ生成部の処理を簡略化すれば暗号化処理速度の低下を小さくすることは可能であるが、その簡略化によって各種解読法、特に既知平文攻撃に対する安全性が低下することになるので、安全性の上で問題である。

そこで、本発明はかかる問題点に鑑みてなされたものであり、鍵更新によって差分解読法・線形解読法といった既知平文攻撃に対する高い安全性を保ちつつ、鍵更新による暗号化処理速度の低下が少ないデータ暗号化装置及び暗号処理方法を提供することを目的とする。

【0 0 2 0】

【課題を解決するための手段】

請求項 1 に係る発明は、入力データを N ビット単位の入力ブロックに分割し、予め与えられた鍵データに基づいて、順次前記入力ブロックを所定のアルゴリズムに従って暗号化し暗号化ブロックとし、前記暗号化ブロックを連結し暗号文データとして出力するデータ暗号化装置であって、

予め初期データが設定されていて、ある入力ブロックに先立ってデータ出力された暗号化ブロックを記憶し、予め設定されている所定の入力ブロックに対して暗号化を行うときには記憶データを前記初期値に初期化するデータ記憶手段と、

前記データ記憶手段の記憶データを所定の変換で変換するデータ変換手段と、

前記データ変換手段から出力されたデータと前記鍵データを融合するデータ融合手段と、

前記所定の入力ブロックに対して暗号化を行う時は前記データ融合手段から出力されたデータに基づいて第 1 の部分鍵生成処理を行い、前記所定の入力ブロック以外の入力ブロックに対して暗号化を行う時は前記データ融合手段から出力されたデータに基づいて第 2 の部分鍵生成処理を行う部分鍵生成手段と、

前記部分鍵生成手段から出力されたデータに基づいて入力ブロックを暗号化して暗号化ブロックとして出力するデータ暗号化手段とを備え、

前記部分鍵生成手段で行う前記第 1 の部分鍵生成処理と前記第 2 の部分鍵生成処理は安全性のための処理負荷を異ならせていることを特徴とする。

#### 【 0 0 2 1 】

請求項 2 に係る発明は、請求項 1 の発明において、前記第 2 の部分鍵生成処理は、前記データ融合手段から出力されたデータに基づいてデータを生成し、前記生成されたデータと同じデータ複数個をビット連結することによって行い、これにより、前記第 1 の部分鍵生成手段よりも安全性のための処理負荷を小さくしていることを特徴とする。

#### 【 0 0 2 2 】

請求項 3 に係る発明は、請求項 1 の発明において、前記データ融合手段におけるデータ融合操作は、ビット毎の排他的論理和、または加算演算とすることを特徴とする。

請求項 4 に係る発明は、請求項 1 の発明において、前記所定の入力ブロックは

、入力されるM番目毎の入力ブロックであって、  
前記数値Mは2以上の整数であることを特徴とする。

【0 0 2 3】

請求項5に係る発明は、入力データをNビット単位の入力ブロックに分割し、  
予め与えられた鍵データに基づいて、順次前記入力ブロックに対して所定の暗号  
化処理を施し暗号化ブロックとし、前記暗号化ブロックを連結し暗号文データと  
して出力する暗号処理方法であって、

記憶手段が、ある入力ブロックに先立ってデータ出力された暗号化ブロックを  
記憶しており、

所定の入力ブロックの暗号処理を行う時は、記憶手段に記憶された連鎖データ  
を所定の初期値に初期化する初期化ステップと、

記憶手段に記憶された連鎖データを所定の変換で変換し変換データを生成する  
データ変換ステップと、

変換データと鍵データを融合して融合データを生成する融合ステップと、

前記所定の入力ブロックの暗号処理を行う時は、前記融合データに基づいて第  
1 部分鍵生成処理を行って部分鍵データを生成し、前記所定の入力ブロック以外  
の入力ブロックの暗号処理を行う時は、前記融合データに基づいて第2 部分鍵生  
成処理を行って部分鍵データを生成する部分鍵生成処理ステップと、

部分鍵データに基づいて入力ブロックを暗号化し暗号化データを生成して暗号  
化ブロックとして出力する暗号化ステップと、

暗号化ステップで生成された暗号化データを新たな連鎖データとして記憶手段  
に記憶された連鎖データを更新し、次の暗号処理に供させる記憶ステップとを備  
え、

前記第1 部分鍵生成処理と前記第2 部分鍵生成処理とは安全性のための処理負  
荷を異ならせていることを特徴とする特徴とする。

【0 0 2 4】

請求項6に係る発明は、請求項5の発明において、前記第2 部分鍵生成処理は  
、融合データに基づいてデータを生成し、前記生成されたデータと同じデータ複  
数個をビット連結することによってデータを生成を行い、これによって、前記第

1 部分鍵生成処理よりも安全性のための処理負荷を小さくしていることを特徴とする。

【0025】

請求項7に係る発明は、請求項5の発明において、前記データ融合ステップにおけるデータ融合操作は、ビット毎の排他的論理和、または加算演算とすることを特徴とする。

請求項8に係る発明は、請求項5の発明において、前記所定の入力ブロックは、入力されるM番目毎の入力ブロックであって、前記数値Mは2以上の整数であることを特徴とする。

【0026】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて詳細に説明する。

通常、データ暗号化装置で暗号化された暗号文データは、暗号化した際の鍵データを、共有しているデータ復号化装置で暗号化変換と逆変換となる演算を施され、平文データとなって出力される。本実施形態では、データ暗号化装置を有する送信機において、ある平文データが暗号化されて暗号文データとなって送信され、その暗号文データがデータ復号化装置を有する受信機で復号化されて平文データとなり出力されるという暗号通信システムとして説明する。

(暗号通信システムの構成)

図1は、本実施形態に係る暗号通信システムの構成を示すブロック図である。

【0027】

この暗号通信システムは、送信機1および受信機2から構成される。

送信機1は、図1に示されるように、データ暗号化装置10及び送信部11を備える。データ暗号化装置10には、64ビットの平文データと64ビットの暗号化鍵データが入力される。この平文データは、ディジタル符号化された音声または画像情報をはじめとするディジタル情報である。また、暗号化鍵データは、予め送信機1と受信機2との間で定めていたものである。これら平文データと鍵データは、データ暗号化装置10に入力され処理を施されて64ビットの暗号文データとなる。一般に、暗号化の対象となる平文データは64ビット以上のデー

タであることが多い。その場合は、平文データを 64 ビット単位に分割して順次データ暗号化装置 10 に入力して暗号化していく。そして、送信部 11 により並列 t の直列変換、変調及び増幅され伝送路 3 を経て受信機 2 に送信される。

#### 【0028】

受信機 2 は、図 1 に示されるように、データ復号化装置 20 及び受信部 21 を備える。データ復号化装置 20 には、受信部 21 を介して受信され 64 ビット毎に直列 t の並列変換された暗号文データが入力されていく。また、予め送信機 1 と受信機 2 で定めている 64 ビットの暗号化鍵データが入力されている。入力される 64 ビット暗号文データは、データ復号化装置 20 で暗号化鍵データに従って処理を施されて復号文データとなる。

(データ暗号化装置 10 の構成)

図 2 は、図 1 に示されるデータ暗号化装置 10 の構成を示すブロック図である。

#### 【0029】

本図において、このデータ暗号化装置 10 は、データ暗号化部 100 と部分鍵データ生成部 101 と、排他的論理和部 102 と、データ変換部 103 と、レジスタ 104 と、カウンタ 105 と、部分鍵データ生成制御部 106 と、レジスタ制御部 107 とを備えている。

部分鍵データ生成部 101 は、予め定められた所定周期  $T$  に対して  $T \times n$  ( $n = 0, 1, \dots$ ) ブロック目の平文を暗号化するときに限り、処理量が通常よりも多い (処理負荷の大きい) 部分鍵生成処理を行い、レジスタ 104 は、 $T \times n$  ( $n = 0, 1, \dots$ ) ブロック目の平文を暗号化するときに限り、レジスタの内容を予め設定されている初期値  $IV$  で初期化することを特徴とする。なお、本実施例では、所定の周期  $T$  を  $2^{10}$  とする。ここで " $\alpha^{\beta}$ " は  $\alpha$  を  $\beta$  乗した値を表す。

#### 【0030】

以下では、各部の処理内容について説明する。

データ暗号化部 100 は、64 ビット毎に分割されて入力される平文データを、部分鍵データ生成部 101 から入力される 32 ビット  $\times$  16 の部分鍵データを



用いて暗号化し、64ビット暗号文データを出力する。

部分鍵データ生成部101は、部分鍵データ生成制御部106から入力される制御信号に従って2つの異なる部分鍵生成処理のうちから1つを選択し、排他的論理和部102より入力される64ビットの入力鍵データに対して、選択された部分鍵データ生成処理を行い、32ビット×16の部分鍵データを生成し、出力する。

#### 【0031】

排他的論理和部102は、データ暗号化装置10の外部から入力される64ビットの暗号化鍵データとデータ変換部103から入力される64ビットデータとのビット毎の排他的論理和演算を行い、演算結果の64ビットデータを入力鍵データとして出力する。

データ変換部103は、レジスタ104から入力される64ビットデータに対して所定のデータ変換処理を行い、変換結果の64ビットデータを出力する。尚、本実施例では所定のデータ変換処理を、上位方向への13ビットローテートシフトとする。

#### 【0032】

レジスタ104は、内部に保管している64ビットデータをデータ変換部103に入力する。また、保管データは予め設定されている初期値IVで初期化されており、データ暗号化部100から64ビット暗号文データの入力があった場合には、保管データをその入力データに更新する。さらに、レジスタ制御部107から制御信号“1”の入力があった場合に限り、保管データを初期値IVに初期化する。

#### 【0033】

カウンタ105は、内部に保管するカウント値が初期値0で初期化されているものとし、データ暗号化部100が64ビット平文データの暗号化処理を実行し、64ビット暗号文データを出力する度にカウント値を1だけ増加させて更新する。但し、カウント値( $2^{10}-1$ )は0に更新されるものとする。

部分鍵データ生成制御部106は、カウンタ105のカウント値が0のときには、部分鍵データ生成部101に制御信号“1”を入力し、0以外ときには

制御信号“0”を入力する。

【0034】

レジスタ制御部107は、カウンタ105のカウント値が0のときには、レジスタ104に制御信号“1”を入力し、レジスタ104を初期値IVで初期化させる。カウント値が0以外のときには、制御信号“0”を入力する。

次に、暗号化する時の動作について述べる。

入力される平文データは64ビットのブロック単位に先頭からP0, P1, …に分割される。そしてP0から順に64ビットの平文データとして、データ暗号化装置10に入力され、64ビットの暗号化鍵データに従い暗号化される。データ暗号化装置10では、入力される64ビットの平文データPt (t=0, 1, …) に対して、以下のような暗号化処理が行われる。

【0035】

暗号化の前に、カウンタ105のカウント値は初期値0に設定され、レジスタ104の保管データは初期値IVに設定されているとする。

まず、部分鍵データ生成制御部106およびレジスタ制御部107は、カウンタ105のカウント値が0のときには、制御信号“1”を部分鍵データ生成部101およびレジスタ104にそれぞれ入力し、カウント値が0以外のときには、制御信号“0”を部分鍵データ生成部101およびレジスタ104にそれぞれ入力する。

【0036】

次に、レジスタ104は、レジスタ制御部107から制御信号“1”が入力されたときに限り、保管データを初期値IVに初期化し、制御信号“0”が入力されたときには、初期化は行わない。その後、レジスタ104は、内部に保管している64ビットデータをデータ変換部103に入力する。

次に、データ変換部103はレジスタ104から入力される64ビットデータをデータ変換し、その変換された64ビットデータを排他的論理和部102に入力する。その後、排他的論理和部102はデータ変換部103より入力される64ビットデータと、64ビットの暗号化鍵データとの排他的論理和演算を行い、その結果の64ビットデータを入力鍵データとして部分鍵データ生成部101に

入力する。

【0037】

次に部分鍵データ生成部101は、排他的論理和部102から入力される64ビット入力鍵データに対して、部分鍵データ生成制御部106から入力される制御信号に従って選択した部分鍵データ生成処理によって32ビット×16の部分鍵データを生成し、生成された部分鍵データをデータ暗号化部100に入力する。

【0038】

その後、データ暗号化部100は、データ暗号化装置10の外部から入力される64ビットの平文データPtに対して、部分鍵データ生成部101から入力される64ビットの部分鍵データ32ビット×16に従って暗号化を行い、その結果の64ビット暗号文データをCtとする。そして、データ暗号化装置10はCtを出力する。カウンタ105は、データ暗号化部100が1ブロックの平文データを暗号化して、64ビットの暗号文データを出力する度に、内部のカウント値を1だけ増加させて更新する。但し、カウント値( $2^{10}-1$ )は0に更新されるものとする。

【0039】

そして、レジスタ104は、保管データをデータ暗号化部100から出力される前記64ビット暗号文データCtに更新する。

以上の操作を繰り返し行い、暗号化処理を行う。

尚、データ暗号化部100としては、従来例2で述べたFEAL暗号方式のデータ暗号化部分を用いるものとする。

(データ復号化装置20の構成)

図3は、図1に示されるデータ復号化装置20の構成を示すブロック図である。

【0040】

本図において、このデータ復号化装置20は、データ復号化部200と部分鍵データ生成部201と、排他的論理和部202と、データ変換部203と、レジ

スタ 2 0 4 と、カウンタ 2 0 5 と、部分鍵データ生成制御部 2 0 6 と、レジスタ制御部 2 0 7 とを備えている。

部分鍵データ生成部 2 0 1 は、予め定められた所定周期  $T$  に対して  $T \times n$  ( $n = 0, 1, \dots$ ) ブロック目の暗号文を復号化するときに関り、処理量が通常よりも多い（処理負荷の大きい）部分鍵生成処理を行い、レジスタ 2 0 4 は、 $T \times n$  ( $n = 0, 1, \dots$ ) ブロック目の暗号文を復号化するときに関り、レジスタの内容を予め設定されている初期値  $IV$  で初期化することを特徴とする。なお、本実施例では、所定の周期  $T$  を  $2^{10}$  とする。

#### 【0041】

データ復号化部 2 0 0 は、64 ビット毎に分割されて入力される暗号文データを、部分鍵データ生成部 2 0 1 から入力される 32 ビット  $\times$  16 の部分鍵データを用いて復号化し、64 ビット平文データを出力する。

部分鍵データ生成部 2 0 1 は、部分鍵データ生成制御部 2 0 6 から入力される制御信号に従って 2 つの異なる部分鍵生成処理のうちから 1 つを選択し、排他的論理和部 2 0 2 より入力される 64 ビットの入力鍵データに対して部分鍵データ生成処理を行い、32 ビット  $\times$  16 の部分鍵データを生成し、出力する。

#### 【0042】

排他的論理和部 2 0 2 は、データ復号化装置 2 0 の外部から入力される 64 ビットの暗号化鍵データとデータ変換部 2 0 3 から入力される 64 ビットデータとのビット毎の排他的論理和演算を行い、演算結果の 64 ビットデータを入力鍵データとして出力する。

データ変換部 2 0 3 は、レジスタ 2 0 4 から入力される 64 ビットデータに対して、所定のデータ変換処理を行い、変換結果の 64 ビットデータを出力する。尚、本実施例では所定のデータ変換処理を、上位方向への 13 ビットローテートシフトとする。

#### 【0043】

レジスタ 2 0 4 は、内部に保管している 64 ビットデータをデータ変換部 2 0 3 に入力する。また、保管データは予め設定されている初期値  $IV$  で初期化されており、一つ前のブロックの復号化の時に入力された 64 ビット暗号文データを

保管している。但し、レジスタ制御部 2 0 7 から制御信号 “1” が入力された場合に限り、保管データを初期値 I V に初期化する。

## 【0 0 4 4】

カウンタ 2 0 5 は、内部に保管するカウンタ値が初期値 0 で初期化されているものとし、データ復号化部 2 0 0 が 6 4 ビット暗号文データの復号化処理を実行し、6 4 ビット平文データを出力する度にカウンタ値を 1 だけ増加させて更新する。但し、カウンタ値 ( $2^{10} - 1$ ) は、0 に更新されるものとする。

部分鍵データ生成制御部 2 0 6 は、カウンタ 2 0 5 のカウンタ値が 0 のときには、部分鍵データ生成部 2 0 1 に制御信号 “1” を入力し、0 以外のときには制御信号 “0” を入力する。

## 【0 0 4 5】

レジスタ制御部 2 0 7 は、カウンタ 2 0 5 のカウンタ値が 0 のときには、レジスタ 2 0 4 に制御信号 “1” を入力し、カウンタ値が 0 以外のときには、制御信号 “0” を入力する。

次に、復号化する時の動作について述べる。

入力される暗号文データは 6 4 ビットのブロック単位に先頭から C 0, C 1, … に分割される。そして C 0 から順に 6 4 ビットの暗号文データとして、データ復号化装置 2 0 に入力され、6 4 ビットの暗号化鍵データに従い復号化される。データ復号化装置 2 0 では、入力される 6 4 ビットの暗号文データ C t ( $t = 0, 1, \dots$ ) に対して、以下のような復号化処理が行われる。

## 【0 0 4 6】

復号化の前に、カウンタ 2 0 5 のカウンタ値は初期値 0 に設定され、レジスタ 2 0 4 の保管データは初期値 I V に設定されているとする。

まず、部分鍵データ生成制御部 2 0 6 およびレジスタ制御部 2 0 7 は、カウンタ 2 0 5 のカウンタ値が 0 のときには、制御信号 “1” を部分鍵データ生成部 2 0 1 およびレジスタ 2 0 4 にそれぞれ入力し、カウンタ値が 0 以外のときには、制御信号 “0” を部分鍵データ生成部 2 0 1 およびレジスタ 2 0 4 にそれぞれ入力する。

## 【0 0 4 7】

次に、レジスタ 2 0 4 は、レジスタ制御部 2 0 7 から制御信号 “1” が入力されたときに限り、保管データを初期値 I V に初期化し、制御信号 “0” が入力されたときには、初期化は行わない。その後、レジスタ 2 0 4 は、内部に保管している 6 4 ビットデータをデータ変換部 2 0 3 に入力する。

次に、データ変換部 2 0 3 はレジスタ 2 0 4 から入力される 6 4 ビットデータをデータ変換し、その変換された 6 4 ビットデータを排他的論理和部 2 0 2 に入力する。その後、排他的論理和部 2 0 2 は、データ変換部 2 0 3 より入力される 6 4 ビットデータと、6 4 ビットの暗号化鍵データとの排他的論理和演算を行い、その結果の 6 4 ビットデータを入力鍵として部分鍵データ生成部 2 0 1 に入力する。

#### 【0 0 4 8】

次に部分鍵データ生成部 2 0 1 は、排他的論理和部 2 0 2 から入力される 6 4 ビットの入力鍵データに対して、部分鍵データ生成制御部 2 0 6 から入力される制御信号に従って選択した部分鍵生成処理によって、3 2 ビット×1 6 の部分鍵データを生成し、生成した部分鍵データをデータ復号化部 2 0 0 に入力する。

その後、データ復号化部 2 0 0 は、データ復号化装置 2 0 の外部から入力される 6 4 ビットの暗号文データ C t に対して、部分鍵データ生成部 2 0 1 から入力される 6 4 ビットの部分鍵データ 3 2 ビット×1 6 に従って復号化を行い、その結果の 6 4 ビット平文データを P t とする。そして、データ復号化装置 2 0 は P t を出力する。

#### 【0 0 4 9】

カウンタ 2 0 5 は、データ復号化部 2 0 0 が 1 ブロックの暗号文データを復号化して、6 4 ビットの平文データを出力する度に、内部のカウント値を 1 だけ増加させて更新する。但し、カウンタ値 ( $2^{10} - 1$ ) は 0 に更新されるものとする。

そして、データ復号化部 2 0 0 でのデータ復号化処理が終わり、平文データが出力された後に、レジスタ 2 0 4 は、保管データを前記 6 4 ビット暗号文データ C t に更新する。

#### 【0 0 5 0】

以上の操作を繰り返し行い、復号化処理を行う。

尚、データ復号化部 2 0 0 には、F E A L 暗号化方式のデータ復号化部を用いるものとする。

(部分鍵データ生成部 1 0 1, 2 0 1 の構成)

図 4 は、図 2, 図 3 に示す部分鍵データ生成部 1 0 1, 2 0 1 の構成の一例を示すブロック図である。尚、部分鍵データ生成部 1 0 1, 2 0 1 は全く同じ構成をとる。

#### 【 0 0 5 1 】

本図において、この部分鍵データ生成部 1 0 1, 2 0 1 は、データ乱数化部 3 0 1 と、乱数化データ保管部 3 0 2 と、段数制御部 3 0 3 とを備えている。

データ乱数化部 3 0 1 は、段数制御部 3 0 3 から入力される 6 4 ビットに対して、所定のデータ乱数化処理を行い、3 2 ビット部分鍵データ S K および 6 4 ビット乱数化データを出力する。尚、3 2 ビット部分鍵データ S K は乱数化データ保管部 3 0 2 に入力され、6 4 ビット乱数化データは段数制御部 3 0 3 に入力される。

#### 【 0 0 5 2 】

段数制御部 3 0 3 は、データ乱数化部 3 0 1 が合計で何回データ乱数化処理を行ったかを制御する。データ乱数化処理の合計回数が所定の回数に満たない場合、段数制御部 3 0 3 は、データ乱数化部 3 0 1 が出力する 6 4 ビット乱数化データを再びデータ乱数化部 3 0 1 に入力し、データ乱数化操作を繰り返し行わせる。但し、データ乱数化部 3 0 1 が 1 回目のデータ乱数化処理を行うときには、部分鍵データ生成部 3 0 0 の外部から入力される 6 4 ビット入力鍵をデータ乱数化部 3 0 1 に入力する。また、所定の回数は、制御信号 “ 1 ” が入力された場合には、1 6 回とし、制御信号 “ 0 ” が入力された場合には、2 回とする。

#### 【 0 0 5 3 】

乱数化データ保管部 3 0 2 は、データ乱数化部 3 0 1 から入力される 3 2 ビット部分鍵データを保管し、データ乱数化部 3 0 1 が所定回数のデータ乱数化処理を実行した後、3 2 ビット×1 6 の部分鍵データを出力する。乱数化データ保管部 3 0 2 は、入力される制御信号によって、以下に示すように異なった処理を行

う。

#### 【0054】

制御信号“1”が入力された場合、乱数化データ保管部302は、データ乱数化部301から最初に入力される32ビット部分鍵データをSK0、2番目に入力される32ビット部分鍵データをSK1、…、16番目に入力される32ビット部分鍵データをSK15として保管し、データ乱数化部301が16回のデータ乱数化処理を終えた後、保管している32ビット×16の部分鍵データSK0、…、SK15を出力する。

#### 【0055】

制御信号“0”が入力された場合、乱数化データ保管部302は、データ乱数化部301から最初に入力される32ビット部分鍵データをSK0、2番目に入力される32ビット部分鍵データをSK1として保管する。データ乱数化部301が2回のデータ乱数化処理を終えた後、 $SK14 = SK12 = SK10 = SK8 = SK6 = SK4 = SK2 = SK0$ 、および、 $SK15 = SK13 = SK11 = SK9 = SK7 = SK5 = SK3 = SK1$ とした32ビット×16の部分鍵データSK0、…、SK15を出力する。

(データ乱数化部301の構成)

図5は、図4に示すデータ乱数化部301の構成の一例を示すブロック図である。

#### 【0056】

本図において、このデータ乱数化部301は、データ攪乱部3010と、排他的論理和部3011とを備えている。

データ攪乱部3010は、32ビットの入力データに対して、データ乱数化部301の外部から入力される64ビットデータの上位32ビットデータに基づいてデータ攪乱操作を行い、その結果の32ビット攪乱データを出力する。

#### 【0057】

排他的論理和部3011は、データ乱数化部301の外部から入力される64ビットデータの上位32ビットデータとデータ攪乱部3010から入力される32ビットデータとのビット毎の排他的論理和演算を行い、その演算結果の32ビ



ットデータを出力する。

データ乱数化部 3 0 1 の動作を以下で説明する。

データ乱数化部 3 0 1 の外部から入力される 6 4 ビットデータは、まず最初に、上位 3 2 ビットを A 1、下位 3 2 ビットを A 0 として、2 つの 3 2 ビットデータ A 1、A 0 に分割される。そして、A 1 は排他的論理和部 3 0 1 1 およびデータ攪乱部 3 0 1 0 に入力され、A 0 はデータ攪乱部 3 0 1 0 に入力されると同時に、そのまま 3 2 ビットデータ B 1 として出力される。データ攪乱部 3 0 1 0 は、3 2 ビットデータ A 0 を 3 2 ビットデータ A 1 に基づいてデータ攪乱し、結果の 3 2 ビット攪乱データを出力する。

#### 【0 0 5 8】

次に、排他的論理和部 3 0 1 1 は、3 2 ビット攪乱データと 3 2 ビットデータ A 1 とのビット毎の排他的論理和演算を行い、演算結果を 3 2 ビットデータ B 0 として出力すると同時に 3 2 ビット部分鍵データとしても出力する。

以上の操作で得られた 3 2 ビットデータ B 1、B 0 について、B 1 を上位 3 2 ビット、B 0 を下位 3 2 ビットとしてビット連結した 6 4 ビットデータを、データ乱数化部 3 0 1 の出力データとして出力する。

#### 【0 0 5 9】

尚、データ攪乱部 3 0 1 0 には、第 2 の従来例で述べた F E A L 暗号方式のデータ攪乱部を用いるものとする。

(暗号通信システムの動作)

次に、上述の図 1 ～図 5 を参照し、本暗号通信システム全体の動作を説明する。

#### 【0 0 6 0】

送信機 1 においては、入力されたデータは 6 4 ビット単位に先頭から P 0、P 1、P 2、…に平文データとして分割される。そして、P 0 から順にデータ暗号化装置 1 0 に入力されて、送信機 1 に予め保持されている 6 4 ビットの暗号化鍵データに従って、暗号化される。暗号化処理は  $(2^{10}) \times k$  ブロック目の平文データの暗号化処理だけが、他の平文ブロックの処理とは異なることを特徴する。但し、 $k = 0, 1, \dots$  とする。具体的には、データ暗号化装置 1 0 では、入

力される平文データ  $P_t$  ( $t = 0, 1, \dots$ ) に対して、以下のような暗号化処理が行われる。

## 【0061】

レジスタ 104 は、レジスタ制御部 107 の制御の下で、 $t$  個目のデータ  $P_t$  を暗号化するときには、以下に示す 64 ビットデータ  $R_{0t}$  を出力する。

$R_{0t} = C(t-1)$  ( $t \neq (2^{10}) \times k, k = 0, 1, \dots$  の場合) …  
………… (式 1)

$R_{0t} = IV$  ( $t = (2^{10}) \times k, k = 0, 1, \dots$  の場合) …………… (式 2)

次に、データ変換部 103 は、レジスタ 104 からの入力に対してデータ変換処理を行い、以下に示す 64 ビットデータ  $S_{0t}$  を出力する。

## 【0062】

$S_{0t} = f(R_{0t})$  …………… (式 3)

但し、 $f(X)$  は入力データ  $X$  に対して、データ変換部 103 でのデータ変換処理を行った結果の値を表す。

次に、排他的論理和部 102 は、データ変換部 103 からの入力に対して、以下に示す 64 ビットデータ  $IK_{0t}$  を出力する。

## 【0063】

$IK_{0t} = S_{0t} (+) EK$  …………… (式 4)

但し、 $EK$  はデータ暗号化装置 10 の外部から入力される、暗号化鍵データであり、“ $(+)$ ” はビット毎の排他的論理和演算を表す。

次に、部分鍵データ生成部 101 は、部分鍵データ生成制御部 106 の制御の下で、排他的論理和部 102 からの入力に対して、以下に示す、32 ビット  $\times$  16 の部分鍵データ  $SK_{0t}$  を出力する。

## 【0064】

$SK_{0t} = KGA(IK_{0t})$  ( $t \neq (2^{10}) \times k, k = 0, 1, \dots$  の場合) …………… (式 5)

$SK_{0t} = KGB(IK_{0t})$  ( $t = (2^{10}) \times k, k = 0, 1, \dots$  の場合) …………… (式 6)

KGA (X) は、入力データ X に対して、部分鍵データ生成制御部 1 0 6 から制御信号 “0” が入力された場合の部分鍵データ生成処理を行った結果の値を表し、KGB (X) は制御信号 “1” が入力された場合の部分鍵データ生成処理を行った結果の値を表す。

## 【0 0 6 5】

次に、データ暗号化部 1 0 0 は、部分鍵データ生成部 1 0 1 からの入力及びデータ暗号化装置 1 0 の外部から入力される平文データ  $P_t$  に対して、以下に示す暗号文データ  $C_t$  を出力する。

$$C_t = \text{Enc} (P_t, SK_{0t}) \quad \dots\dots\dots (\text{式 } 7)$$

送信部 1 1 では、 $C_0, C_1, \dots$  を先頭から連結して暗号文データとして受信機 2 に送信する。

## 【0 0 6 6】

受信機 2 においては、入力されたデータは 6 4 ビット単位に先頭から  $C_0, C_1, C_2, \dots$  の順に暗号文データとして分割される。そして、 $C_0$  から順にデータ復号化装置 2 0 に入力されて、受信機 2 に予め保持されている 6 4 ビットの暗号化鍵データを用いて、復号化される。

データ復号化装置 2 0 では、入力される暗号文データ  $C_t$  ( $t = 0, 1, \dots$ ) に対して、以下のような復号化処理が行われる。

レジスタ 2 0 4 は、レジスタ制御部 2 0 7 の制御の下で、 $t$  個目のデータ  $E_t$  を復号化するときには、以下に示す 6 4 ビットデータ  $R_{1t}$  を出力する。

## 【0 0 6 7】

$$R_{1t} = C(t-1) \quad (t \neq (2^{10}) \times k, k = 0, 1, \dots \text{の場合}) \quad \dots\dots\dots (\text{式 } 8)$$

$$R_{1t} = IV(t = (2^{10}) \times k, k = 0, 1, \dots \text{の場合}) \quad \dots\dots\dots (\text{式 } 9)$$

次に、データ変換部 2 0 3 は、レジスタ 2 0 4 からの入力に対してデータ変換処理を行い、以下に示す 6 4 ビットデータ  $S_{1t}$  を出力する。

## 【0 0 6 8】

$$S_{1t} = f(R_{1t}) \quad \dots\dots\dots (\text{式 } 10)$$

但し、 $f(X)$  は入力データ  $X$  に対して、データ変換部 2 0 3 でのデータ変換処理を行った結果の値を表す。

次に、排他的論理和部 2 0 2 は、データ変換部 2 0 3 からの入力に対して、以下に示す 6 4 ビットデータ  $IK1t$  を出力する。

【0 0 6 9】

$$IK1t = S1t (+) EK \quad \dots\dots\dots (式 1 1)$$

但し、 $EK$  はデータ復号化装置 2 0 の外部から入力される、暗号化鍵データであり、“ $(+)$ ” はビット毎の排他的論理和演算を表す。

次に、部分鍵データ生成部 2 0 1 は、部分鍵データ生成制御部 2 0 6 の制御の下で、排他的論理和部 2 0 2 からの入力に対して、以下に示す 3 2 ビット  $\times$  1 6 の部分鍵データ  $SK1t$  を出力する。

【0 0 7 0】

$$SK1t = KGA (IK1t) \quad (t \neq (2^{10}) \times k, k = 0, 1, \dots \text{の場合}) \quad \dots\dots\dots (式 1 2)$$

$$SK1t = KGB (IK1t) \quad (t = (2^{10}) \times k, k = 0, 1, \dots \text{の場合}) \quad \dots\dots\dots (式 1 3)$$

$KGA(X)$  は、入力データ  $X$  に対して、部分鍵データ生成制御部 2 0 6 から制御信号 “0” が入力された場合の部分鍵データ生成処理を行った結果の値を表し、 $KGB(X)$  は制御信号 “1” が入力された場合の部分鍵データ生成処理を行った結果の値を表す。

【0 0 7 1】

次に、データ復号化部 2 0 0 は、部分鍵データ生成部 2 0 1 からの入力及びデータ復号化装置 2 0 の外部から入力される暗号文データ  $E t$  に対して、以下に示す復号文データ  $D t$  を出力する。

$$D t = Dec (C t, SK1t) \quad \dots\dots\dots (式 1 4)$$

平文データ列  $P 0, P 1, \dots$  に対して、6 4 ビットの暗号化鍵データを用いて暗号化した暗号文データ列  $C 0, C 1, \dots$  を同じ 6 4 ビットの暗号化鍵データを用いてデータ復号化装置 2 0 で復号した復号文データ  $D 0, D 1, \dots$  は、平文データ  $P 0, P 1, \dots$  に等しい。次にそのことを示す。

## 【0072】

(式1)，(式2)及び(式8)，(式9)より、

$$R0t = R1t \quad (t = 0, 1, \dots) \quad \dots\dots\dots (式15)$$

が成り立つ。この(式15)と(式3)，(式10)から、

$$S0t = S1t \quad (t = 0, 1, \dots) \quad \dots\dots\dots (式16)$$

が成り立つ。次に、この(式16)と(式4)，(式11)とから、

$$IK0t = IK1t \quad (t = 0, 1, \dots) \quad \dots\dots\dots (式17)$$

が成り立つ。よって、この(式17)および(式5)，(式6)，(式12)，  
(式13)から

$$SK0t = SK1t \quad (t = 0, 1, \dots) \quad \dots\dots\dots (式18)$$

が成り立つ。ここで、(式7)，(式14)から、

$$Dt = Dec(Enc(Pt, SK0t), SK1t) \quad (t = 0, 1, \dots) \\ \dots\dots\dots (式19)$$

が成り立つが、Enc，Decについては、任意の64ビットデータ $\alpha$ ， $\beta$ について、以下のような関係式(式20)が成り立つ

$$\alpha = Dec(Enc(\alpha, \beta), \beta) \quad \dots\dots\dots (式20)$$

よって、(式19)，(式20)及び(式18)から、

$$Dt = Pt$$

が成り立つことがいえる。

## 【0073】

次に本データ暗号化装置10の安全性及について述べる。本データ暗号化装置10の安全性はデータ暗号化部101の安全性に大きく依存している。本実施形態の場合、データ暗号化部101へ入力される入力鍵データIK0tは、各64ビットの平文データPtの暗号化毎に更新していくので、第3の従来例と同様、入力鍵データを全て同じとする第2の従来例と比べて安全性が向上している。

$t \neq (2^{10}) \times k$  ( $k = 0, 1, \dots$ ) なる平文ブロックPtの暗号化では、データ暗号化部100に入力される32ビット $\times$ 16の部分鍵データSK0， $\dots$ ，SK15については、 $SK0 = SK2 = \dots = SK14$  及び  $SK1 = SK3 = \dots = SK15$  であることから、SK0，SK1， $\dots$ ，SK15の値がすべて異なる

場合と比べて既知平文攻撃に対する安全性は弱くなる。しかし、それらの平文ブロックの暗号化で用いられる入力鍵データ  $IKOt$  は、

$$IKOt = EK(+)(C(t-1))$$

となり、その中で同じ  $IKOt$  を用いて暗号化されている平文ブロックを大量に収集することは、 $C(t-1)$  が  $2^{64}$  通り（ここで  $\alpha^{\beta}$  は  $\alpha$  を  $\beta$  乗した値を表す）の値を取りうることからほとんど不可能に近いといえる。よって、この方法による既知平文攻撃は成功しない。

#### 【0074】

一方、 $t = (2^{10}) \times k$  ( $k = 0, 1, \dots$ ) なる平文ブロック  $Pt$  の暗号化では、データ暗号化部 100 に入力される 32 ビット  $\times$  16 の部分鍵データ  $SK0, \dots, SK15$  は、全て異なる値となるように生成されるので、この方法による既知平文攻撃の安全性は、第 3 の従来例と全く同じになる。

次に本データ暗号化装置 10 の暗号化処理速度性能について述べる。

$t \neq (2^{10}) \times k$  ( $k = 0, 1, \dots$ ) なる平文ブロック  $Pt$  の暗号化では、部分鍵データ生成部 101 は、実質は 32 ビット  $\times$  2 の部分鍵データを生成しているのと同じである簡便な処理によって部分鍵生成データ 32 ビット  $\times$  16 を生成しているので、各ブロック毎に部分鍵データを生成することによる、暗号化処理速度の低下は、第 3 の従来例よりも少なく済む。

#### 【0075】

なお、本実施形態においては、データ変換部 103, 203 の 64 ビット出力データと、暗号化鍵データとの融合手段として、ビット毎の排他的論理和演算を用いているが、これはビット毎の排他的論理和でなくても、同様な効果が得られる。

また、本実施形態においては、データ変換部 103, 203 から出力される変換データは 64 ビットとしているが、これは 64 ビットである必要はない。例えば、暗号化鍵データが 56 ビットである場合には、出力データが 56 ビットとなるようなデータ変換部を用いれば良い。

#### 【0076】

また、本実施形態においては、レジスタ 104, 204 に 1 つ前の暗号化で生

成される暗号文データを入力しているが、これは1つ前の暗号化の処理過程で得られる64ビットの値であれば何でもよい。さらにこの値は、64ビットである必要はなく、64ビット以下、例えば40ビットといった場合には、入力データが40ビットとなるようなデータ変換手段を、データ変換部103, 203に用いればよい。

## 【0077】

また、本実施形態においては、データ暗号化部100としてFEAL暗号方式を用いているが、これはブロック暗号方式であれば何でもよい。

また、部分鍵データ生成部101は、本実施形態に用いた構成に限定されるものではなく、64ビットの入力鍵データから、32ビット×16の部分鍵データを生成するものであればよい。

## 【0078】

また、部分鍵データ生成部101で用いる異なる2種類の暗号化処理は、本実施形態に用いた様な乱数化の処理量を異ならせる構成に限定されるものではなく、制御信号“1”が入力された時に選択される暗号化処理が、制御信号“0”が入力された時に選択される暗号化処理よりも処理負荷の大きいものであれば何でもよい。

## 【0079】

また、カウンタ105, 205はカウント値( $2^{10}-1$ )を0に更新するものとしているが、これは、( $2^{10}-1$ )という値に制限されるものではなく、任意の正の整数であれば何でもよいし、0への更新を行わなくてもよい。

また、本実施形態では、64ビットの暗号化鍵データを装置内に保管しているが、これは最初の暗号化に用いる64ビットの暗号化鍵データを最初に保管しておき、残りの暗号化鍵データは暗号化されて平文データと共に伝送するようにするか、実鍵データを更新する度に、例えば、Diffie-Hellman方式などの公開鍵暗号方式を用いて、暗号化鍵データを配送し、共有するようにしてもよい。

## 【0080】

## 【発明の効果】

以上の説明から明らかなように、本発明は、入力データをNビット単位の入力ブロックに分割し、予め与えられた鍵データに基づいて、順次前記入力ブロックを所定のアルゴリズムに従って暗号化し暗号化ブロックとし、暗号化ブロックを連結し暗号文データとして出力するデータ暗号化装置であって、

予め初期データが設定されていて、ある入力ブロックに先立ってデータ出力された暗号化ブロックを記憶し、予め設定されている所定の入力ブロックに対して暗号化を行うときには記憶データを初期値に初期化するデータ記憶手段と、

データ記憶手段の記憶データを所定の変換で変換するデータ変換手段と、

データ変換手段から出力されたデータと鍵データを融合するデータ融合手段と

、  
所定の入力ブロックに対して暗号化を行う時はデータ融合手段から出力されたデータに基づいて第1の部分鍵生成処理を行い、所定の入力ブロック以外を入力ブロックに対して暗号化を行う時はデータ融合手段から出力されたデータに基づいて第2の部分鍵生成処理を行う部分鍵生成手段と、

部分鍵生成手段から出力されたデータに基づいて入力ブロックを暗号化して暗号化ブロックとして出力するデータ暗号化手段とを備え、

部分鍵生成手段で行う第1の部分鍵生成処理と第2の部分鍵生成処理は安全性のための処理負荷を異ならせているため、従来の様に全ての入力ブロックに対して安全性のための処理負荷の大きい部分鍵生成を行うのではなく、ある特定の入力ブロックに対してのみ安全性のための処理負荷の大きい部分鍵生成を行い、これにより、処理速度の低下を少なくして、暗号の安全性を高めることが可能である。

【0081】

よって、本発明によれば従来と同様の安全性向上の効果を得ながらも、従来よりも高速な暗号処理を実現するものであり、特にマルチメディア技術の進展が望まれる今日における画像情報等のリアルタイム秘密通信等に好適であり、その実用効果は極めて大きい。

【図面の簡単な説明】

【図1】



本発明の実施形態に係る暗号通信システムの構成を示すブロック図

【図 2】

同データ暗号化装置 1 0 の構成を示すブロック図

【図 3】

同データ復号化装置 2 0 の構成を示すブロック図

【図 4】

同部分鍵データ生成部 1 0 1, 2 0 1 の構成を示すブロック図

【図 5】

同データ乱数化部 3 0 1 の構成を示すブロック図

【図 6】

従来 of データ暗号化装置の構成を示すブロック図

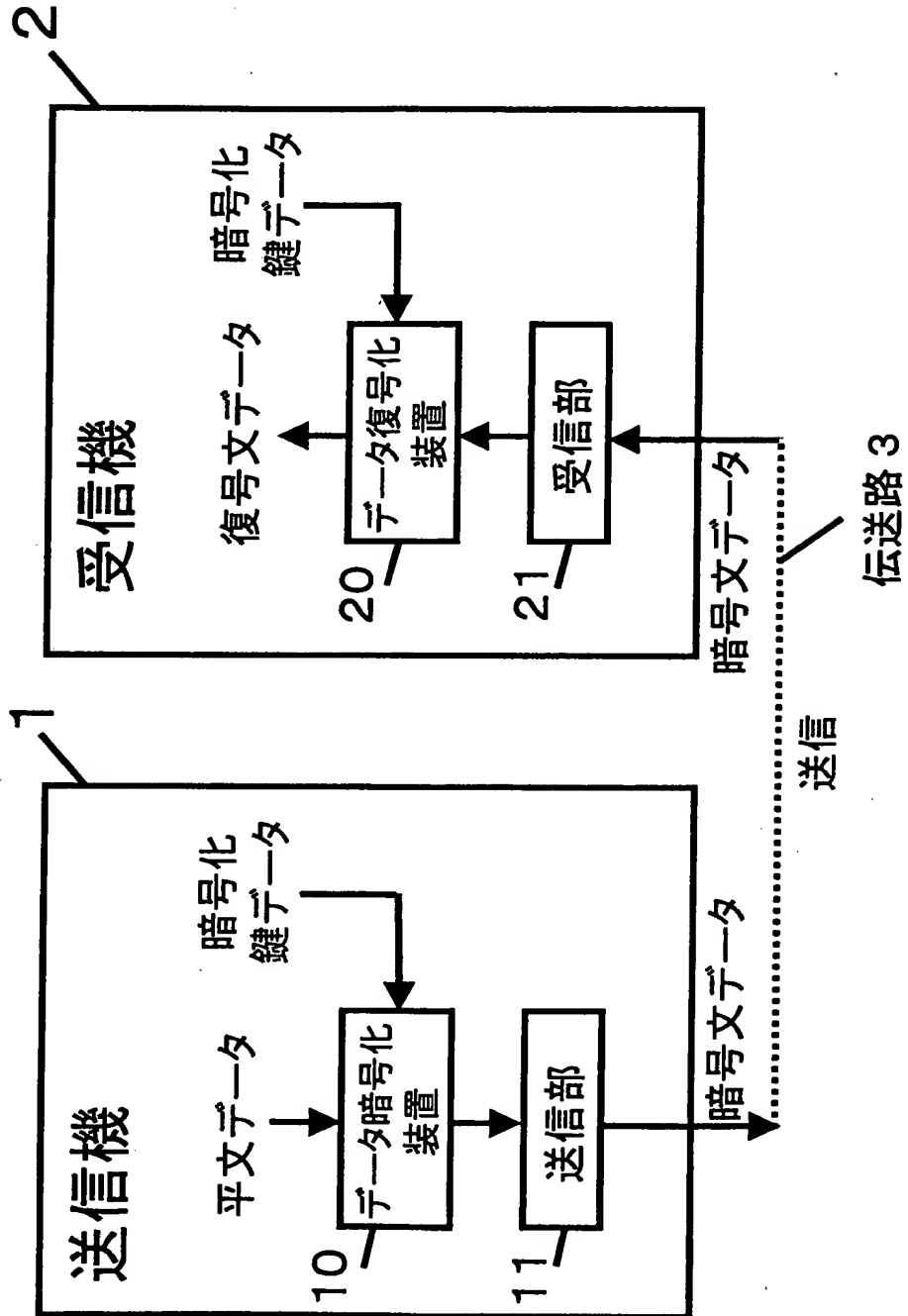
【符号の説明】

- 1        送信機
- 2        受信機
- 3        伝送路
- 1 0      データ暗号化装置
- 1 1      送信部
- 2 0      データ復号化装置
- 2 1      受信部
- 1 0 0    データ暗号化部
- 1 0 1    部分鍵データ生成部
- 1 0 2    排他的論理和部
- 1 0 3    データ変換部
- 1 0 4    レジスタ
- 1 0 5    カウンター
- 1 0 6    部分鍵データ生成制御部
- 1 0 7    レジスタ制御部

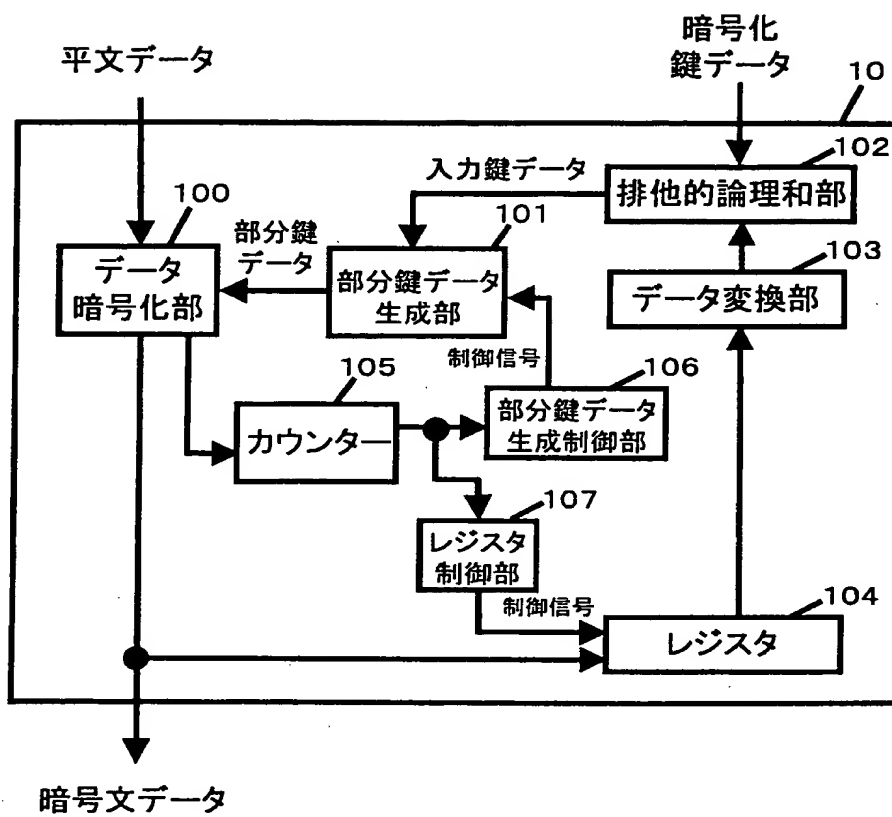
【書類名】

図面

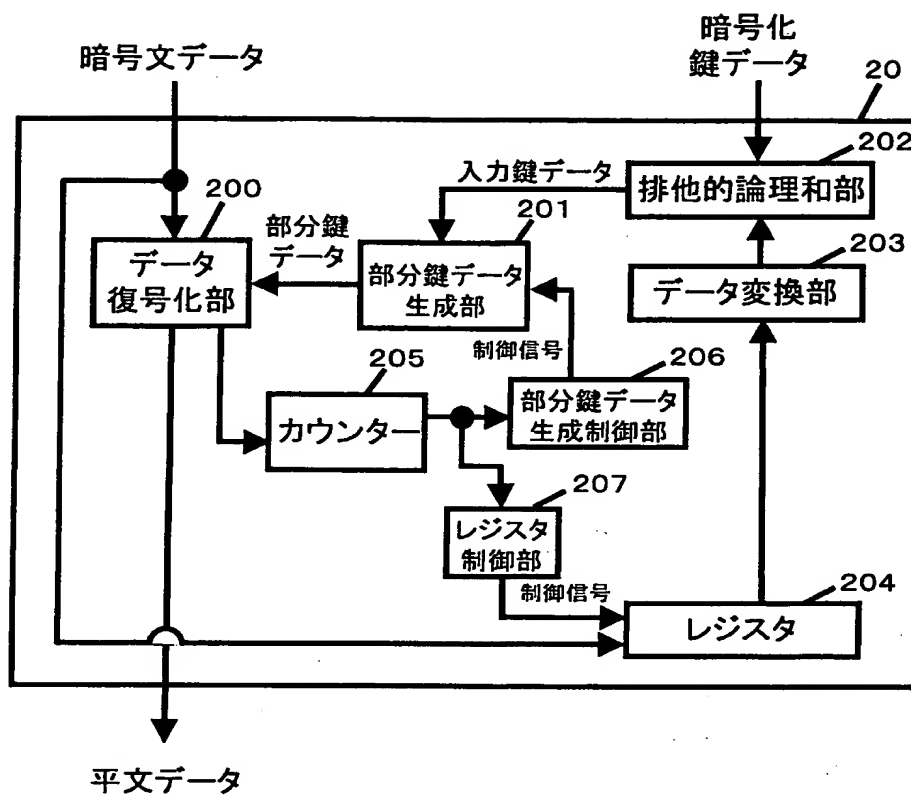
【図 1】



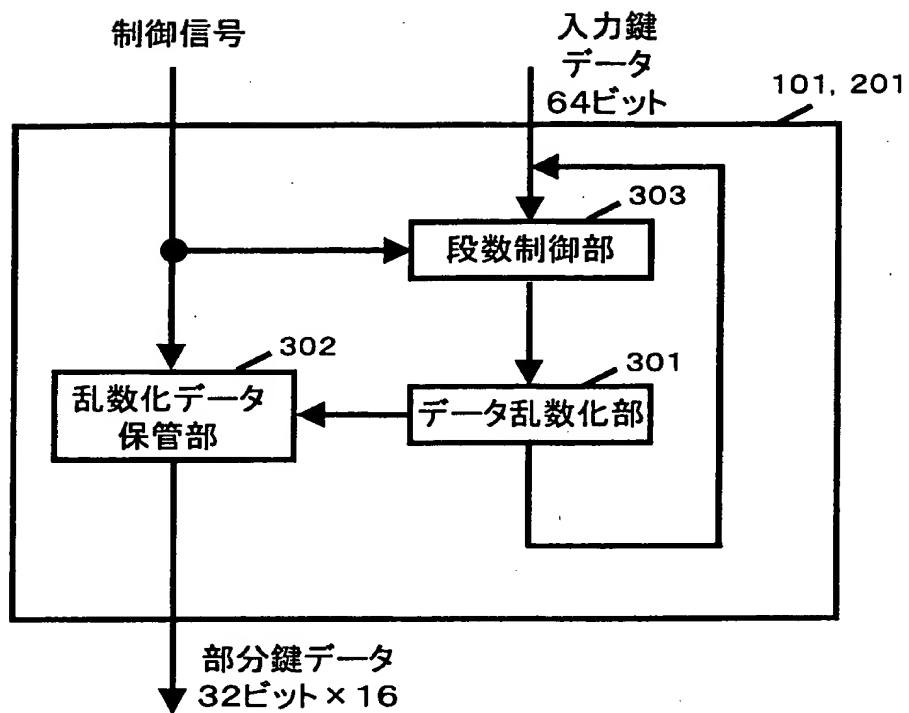
【図 2】



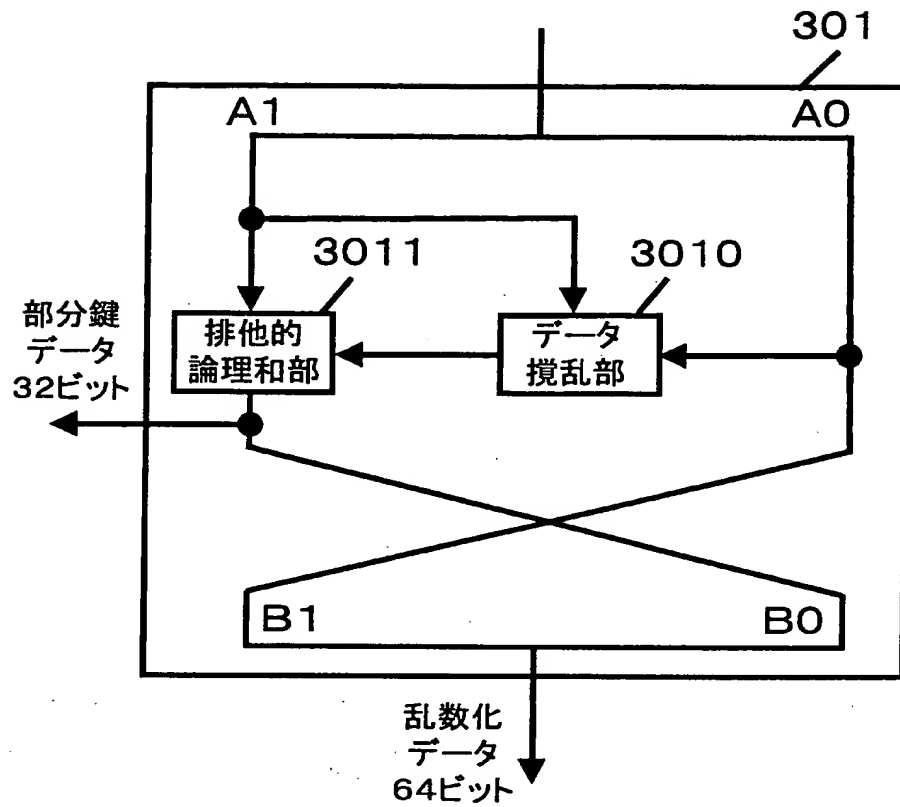
【図 3】



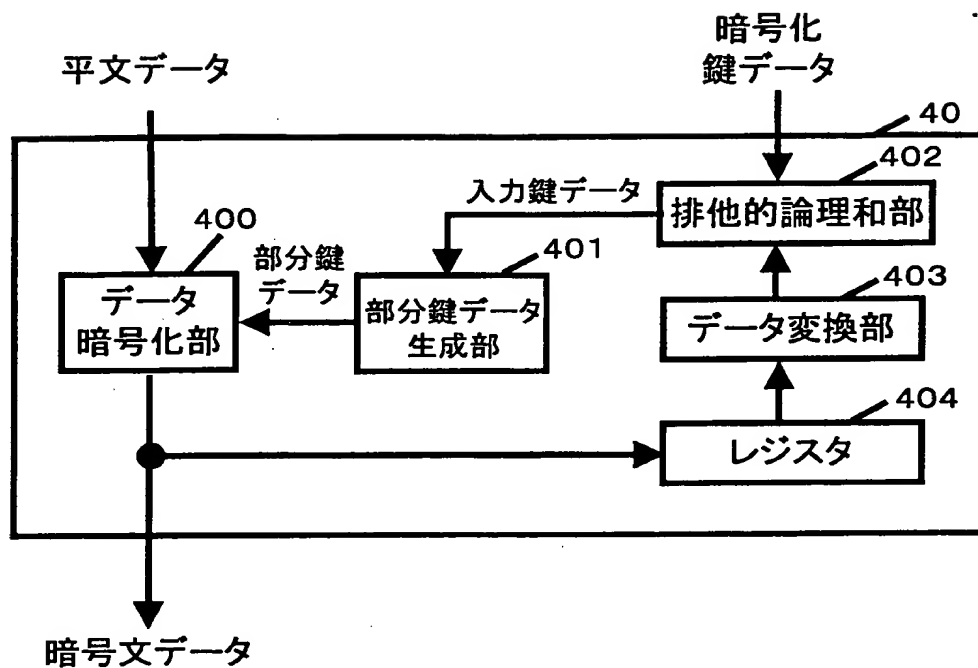
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 直前の平文ブロックから得られる可変情報を用いて鍵データを更新していく暗号方式は、安全性の向上が実現できる一方、1ブロック暗号化を行う毎に部分鍵生成を行うことから、処理速度が大幅に低下する。

【解決手段】 特定の平文ブロックの暗号化には、安全性のための処理負荷の大きい部分鍵生成処理を行い、それ以外の平文ブロックの暗号化には、処理負荷の小さい部分鍵生成処理を行うことで、処理速度低下が少なく、安全性の向上したデータ暗号化装置、暗号処理方法を実現する。

【選択図】 図2



出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝